IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS

TRANQUILITY IP LLC, Plaintiff, v. **TELLABS BROADBAND LLC,** Defendant.	C.A. No. 3:22-cv-1925 **JURY TRIAL DEMANDED** **PATENT CASE**

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Tranquility IP LLC files this Original Complaint for Patent Infringement against Tellabs Broadband LLC and would respectfully show the Court as follows:

I. THE PARTIES

1. Plaintiff Tranquility IP LLC ("Tranquility" or "Plaintiff") is a Texas limited liability company having an address at 7548 Preston Rd, Suite 141 PMB 1114, Frisco, TX 75034.

2. On information and belief, Defendant Tellabs Broadband LLC ("Defendant") is a limited liability company with its principal place of business at 4240 International Parkway, Suite 105, Carrollton, TX 75007. Defendant has a registered agent at National Registered Agents, Inc., 1999 Bryan St., Suite 900, Dallas, TX 75201.

II. JURISDICTION AND VENUE

3. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has subject matter jurisdiction of such action under 28 U.S.C. §§ 1331 and 1338(a).

4. On information and belief, Defendant is subject to this Court's specific and general personal jurisdiction, pursuant to due process and the Texas Long-Arm Statute, due at least to its

business in this forum, including at least a portion of the infringements alleged herein at 4240 International Parkway, Suite 105, Carrollton, TX 75007.

5. Without limitation, on information and belief, within this state, Defendant has used the patented inventions thereby committing, and continuing to commit, acts of patent infringement alleged herein. In addition, on information and belief, Defendant has derived revenues from its infringing acts occurring within Texas. Further, on information and belief, Defendant is subject to the Court's general jurisdiction, including from regularly doing or soliciting business, engaging in other persistent courses of conduct, and deriving substantial revenue from goods and services provided to persons or entities in Texas. Further, on information and belief, Defendant is subject to the Court's personal jurisdiction at least due to its sale of products and/or services within Texas. Defendant has committed such purposeful acts and/or transactions in Texas such that it reasonably should know and expect that it could be haled into this Court as a consequence of such activity.

6. Venue is proper in this district under 28 U.S.C. § 1400(b). On information and belief, Defendant maintains its principal place of business in Texas at 4240 International Parkway, Suite 105, Carrollton, TX 75007. On information and belief, from and within this District Defendant has committed at least a portion of the infringements at issue in this case.

7. For these reasons, personal jurisdiction exists and venue is proper in this Court under 28 U.S.C. § 1400(b).

III. COUNT I
(PATENT INFRINGEMENT OF UNITED STATES PATENT NO. 8,272,037)

8. Plaintiff incorporates the above paragraphs herein by reference.

9. On September 18, 2012, United States Patent No. 8,272,037 ("the '037 Patent") was duly and legally issued by the United States Patent and Trademark Office. The '037 Patent is titled "Flexible WLAN Access Point Architecture Capable of Accommodating Different User

Devices." A true and correct copy of the '037 Patent is attached hereto as Exhibit A and incorporated herein by reference.

10. Plaintiff is the assignee of all right, title and interest in the '037 patent, including all rights to enforce and prosecute actions for infringement and to collect damages for all relevant times against infringers of the '037 Patent. Accordingly, Plaintiff possesses the exclusive right and standing to prosecute the present action for infringement of the '037 Patent by Defendant.

11. The invention in the '037 Patent relates to the field of controlling access by a mobile terminal to a WLAN by accommodating for the particular capabilities of each mobile terminal and selecting accordingly the optimum available authentication mechanism. (*Id.* at col. 1:17-23).

12. The context of the patented invention in the '037 Patent is wireless local area networks ("WLAN") employing the IEEE 802.1X architecture with an access point that provides access for mobile devices to other networks, such as hardwired local area and global networks such as the Internet. (*Id.* at col. 1:27-31). Because a public WLAN is relatively easy and low cost to implement and operate, it is an ideal access mechanism through which mobile wireless communication devices can exchange packet with an external entity. (*Id.* at col. 1:38-43). WLAN technology has resulted in publicly available hotspots (such as at cafes, restaurants, and libraries) where a mobile device (such as your mobile phone or laptop computer) can access the Internet through an access point associated with a WLAN. (*Id.* at col. 1:32-38). However, such a public deployment can compromise security unless there are adequate means for identification and authentication of connected devices. (*Id.* at col. 1:43-46).

13. When a mobile device incorporating an IEEE 802.1X protocol ("IEEE 802.1X client") attempts to access a public WLAN or hotspot, the IEEE 802.1X client would begin the authentication process according to its current machine configurations. (*Id.* at col. 1:47-51). After

authentication occurs, the public WLAN opens a secure data channel to a mobile communications device to protect the privacy of data passing between the WLAN and the device. (*Id.* at col. 1:51-54). Although many manufacturers of WLAN equipment have adopted the IEEE 802.1X protocol for deployed equipment, other devices using WLAN may use other protocols such as may be provided by wired electronic privacy ("WEP"). (*Id.* at col. 1:54-58). Unfortunately, the IEEE 802.1X protocol was designed with a private LAN access as its usage model so the protocol does not provide certain features necessary for a public WLAN environment. (*Id.* at col. 1:60-64). For example, the IEEE 802.1X protocol does not have a sophisticated mechanism for interacting with users. (*Id.* at col. 1:65-col. 2:1). The access point can only send simple messages to the client using electronic access point notification. (*Id.* at col. 2:1-3). This may be sufficient for an enterprise setting but would be insufficient for a public hotspot. (*Id.* at col. 2:3-5). A public hotspot should therefore be able to accommodate different client and operator capabilities, based on which the WLAN should have the ability to select different authentication mechanism. (*Id.* at col. 2:25-28). The prior art does not sufficiently address how the systems would provide such capabilities. (*Id.* at col. 2:28-31). The invention in the '037 patent seeks to address the variation in authentication mechanisms by providing a method for controlling the access of a terminal device in a WLAN environment by determining whether a terminal device uses an IEEE 802.1X protocol. (*Id.* at col. 2:43-46).

14. **Direct Infringement.** Upon information and belief, Defendant has been directly infringing at least claims 9, 10, and 11 of the '037 patent in Texas, and elsewhere in the United States, by performing actions comprising at least performing the claimed method of controlling access by a user terminal in a wireless local area network by determining whether the user terminal

uses an IEEE 802.1X protocol using at least the Tellabs Flexsym Optical Network Terminal 205 ("Accused Instrumentality") (*e.g.*, https://www.tellabs.com/product/ont205).

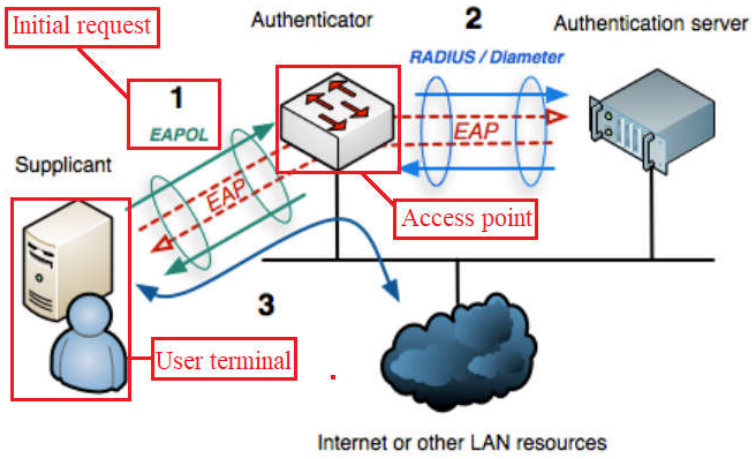
15. The Accused Instrumentality discloses a method for controlling access by a user terminal (*e.g.*, user equipment) in a wireless local area network by determining whether the user terminal utilizes an IEEE 802.1x protocol. IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN. The Accused Instrumentality determines whether the UE supports the IEEE 802.1x protocol by sending an EAP request and waits for response from the UE. If UE responds by authenticating itself using credentials before time out, then it is 802.1x compliant otherwise not.

(*E.g.*, https://www.tellabs.com/product/ont205).

Centralized Management

All features and functionality can be defined in software and dynamically allocated, based on real-time needs. Being controlled by the Tellabs Panorama PON Manager helps speed installations and daily operations. Centrally controlled by the Panorama PON Manager, the Tellabs ONT205 supports auto-discovery mechanisms, can be quickly provisioned using global templates and profiles, and offers smart troubleshooting tools, all of which allow for speedy moves, adds and changes for everyday operations.

(*E.g.*, https://www.tellabs.com/product/ont205).



802.1X authentication involves three parties: a *supplicant*, an *authenticator*, and an *authentication server*. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.

(*E.g.*, https://docs.tellabs.com/articles/#!optical-lan-application-notes-publication/eng-010428-configuring-policy-via-radius-authenticationv4).

Enable 802.1x Authorization

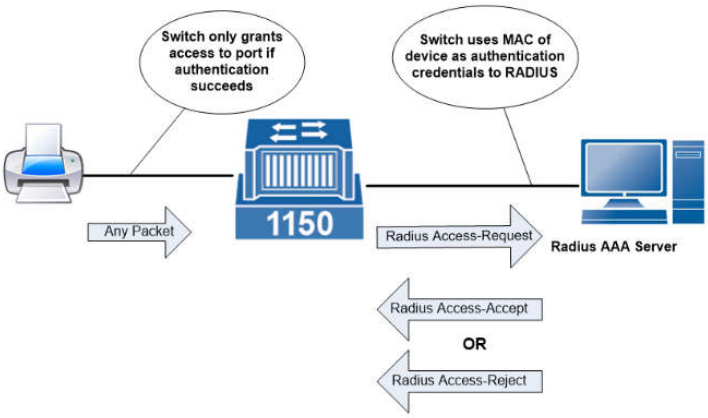
The next step is to configure the system to enable 802.1x Authentication. The system will not do any 802.1x unless this is configured. The 802.1x Port Authentication settings are reached by right clicking on the OLT within the common tree, then selecting the menu item Protocols->Port Authentication.

You should click the checkbox "Enable 802.1x Port Based Access Control".

It is also a good idea to set up the Radius server IP address(es) and Shared Key. This defines the values for the Radius Profile named "default".

(*E.g.*, https://docs.tellabs.com/articles/#!optical-lan-application-notes-publication/eng-010428-configuring-policy-via-radius-authenticationv4).

MAC Authentication Bypass Described



Many Enterprise and other secure installations use the 802.1x Port Authentication feature to control access to the Ethernet ports within a facility. The 802.1x protocol forces a user to authenticate using their credentials prior to gaining access to a port. The user is typically authenticated to some backend system such as RADIUS.

For many intelligent devices that support 802.1x this works well to secure the ports for use only by authorized parties. The problem is that there are simple devices such as printers and cameras that may not support 802.1x and backend authorization. In order to handle these use cases, the feature of MAC Authentication Bypass or MAB uses the MAC address of the attached device to authenticate to the backend AAA server, typically RADIUS.

(*E.g.*, https://docs.tellabs.com/articles/#!optical-lan-application-notes-publication/eng-010469-mac-authentication-bypass).

Mixing of 802.1x and MAB

MAB and 802.1x can both be configured onto the port. The default settings will allow 802.1x to be tried first, followed by an attempt with MAB using the device's MAC address. An entire site can be configured this way to allow the 802.1x or MAB devices to be plugged into any port on the OLT. This can also be used for example to authenticate phones that don't support 802.1x but force PCs to authenticate.

It should be noted that if multiple devices are attempting access on the same port the 802.1x supplicants will ALWAYs be given preference over MAB clients.

(*E.g.*, https://docs.tellabs.com/articles/#!optical-lan-application-notes-publication/eng-010469-mac-authentication-bypass).

To enable MAB you need to change the following settings in the NAC profile:

- **MAC-BYPASS** – Should be set to enabled to turn on MAC Bypass.
- **Startup Delay** – Defaults to 30 seconds to give standard 802.1x time to complete prior to MAB being attempted. Always best to let 802.1x be attempted first, but some devices may need a shorter timer to speed up access to the network.
- **Authentication Method** – Set to PAP if your Radius server is set up to accept PAP.

(*E.g.*, https://docs.tellabs.com/articles/#!optical-lan-application-notes-publication/eng-010469-mac-authentication-bypass).

Authentication Timeout in 802.1x

-> By using Authentication Timeout Switch knows whether the end device which is connected to an interface is having 802.1x supplicant or not.

-> By default Switch sends EAP request identity messages every 30 seconds to the endpoint, if the switch does not receive the response for three EAP request identity messages (90 seconds) then it assumes the host is not having 802.1x supplicant and begins MAB process.

-> It is recommended to change the Authentication timeout period to less value.

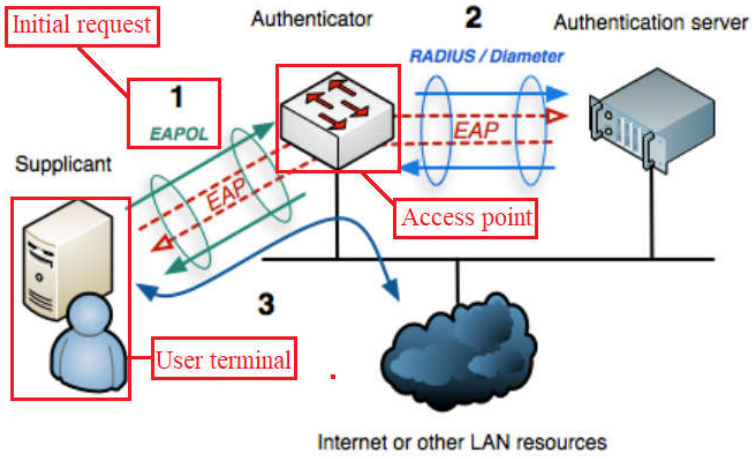
(*E.g.*, https://www.kareemccie.com/2017/01/mac-authentication-bypass.html).

16. Upon information and belief, the Accused Instrumentality is used in a method performing the step of an access point (*e.g.*, authenticator) communicating to the user terminal (*e.g.*, user equipment) a request (*e.g.*, EAPoL request) to identify (*e.g.*, to identify whether UE is a supplicant or not), and if the user terminal utilizes an IEEE 802.1x protocol, acknowledging the request to identify (*e.g.*, when UE supports 802.1x, it authenticates itself using credentials), otherwise the access point determining that the user terminal is not IEEE 802.1x compliant and selecting an authentication mechanism (*e.g.*, Mac Authentication Bypass or MAB) compatible with the user terminal.

tellabs® HOME SOLUTIONS PRODUCTS SERVICES PARTNERS

- Network Access Control (NAC)
- IGMP v2/v3 snooping
- IEEE 802.1x Port-Based Authentication/MAB
- Link Layer Data Protocol (LLDP) for autoprovisioning, inventory and PoE power management.

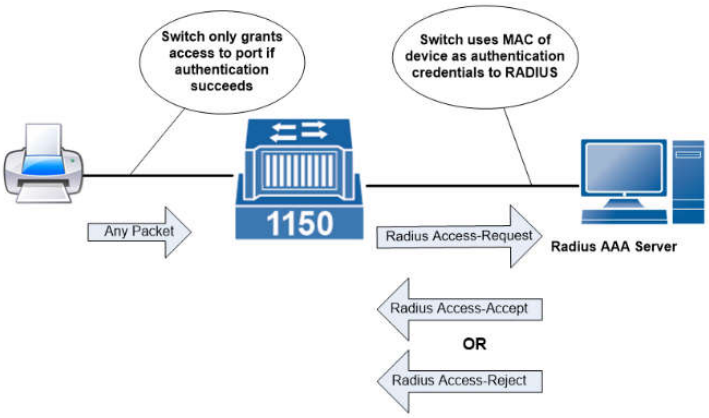
(*E.g.*, https://www.tellabs.com/product/ont205).



802.1X authentication involves three parties: a *supplicant*, an *authenticator*, and an *authentication server*. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.

(*E.g.*, https://docs.tellabs.com/articles/#!optical-lan-application-notes-publication/eng-010428-configuring-policy-via-radius-authenticationv4).

MAC Authentication Bypass Described



Many Enterprise and other secure installations use the 802.1x Port Authentication feature to control access to the Ethernet ports within a facility. The 802.1x protocol forces a user to authenticate using their credentials prior to gaining access to a port. The user is typically authenticated to some backend system such as RADIUS.

For many intelligent devices that support 802.1x this works well to secure the ports for use only by authorized parties. The problem is that there are simple devices such as printers and cameras that may not support 802.1x and backend authorization. In order to handle these use cases, the feature of MAC Authentication Bypass or MAB uses the MAC address of the attached device to authenticate to the backend AAA server, typically RADIUS.

Mixing of 802.1x and MAB

MAB and 802.1x can both be configured onto the port. The default settings will allow 802.1x to be tried first, followed by an attempt with MAB using the device's MAC address. An entire site can be configured this way to allow the 802.1x or MAB devices to be plugged into any port on the OLT. This can also be used for example to authenticate phones that don't support 802.1x but force PCs to authenticate.

It should be noted that if multiple devices are attempting access on the same port the 802.1x supplicants will ALWAYs be given preference over MAB clients.

(*E.g.*, https://docs.tellabs.com/articles/#!optical-lan-application-notes-publication/eng-010469-mac-authentication-bypass).

To enable MAB you need to change the following settings in the NAC profile:

- **MAC-BYPASS** – Should be set to enabled to turn on MAC Bypass.
- **Startup Delay** – Defaults to 30 seconds to give standard 802.1x time to complete prior to MAB being attempted. Always best to let 802.1x be attempted first, but some devices may need a shorter timer to speed up access to the network.
- **Authentication Method** – Set to PAP if your Radius server is set up to accept PAP.

(*E.g.*, https://docs.tellabs.com/articles/#!optical-lan-application-notes-publication/eng-010469-mac-authentication-bypass).

Authentication Timeout in 802.1x

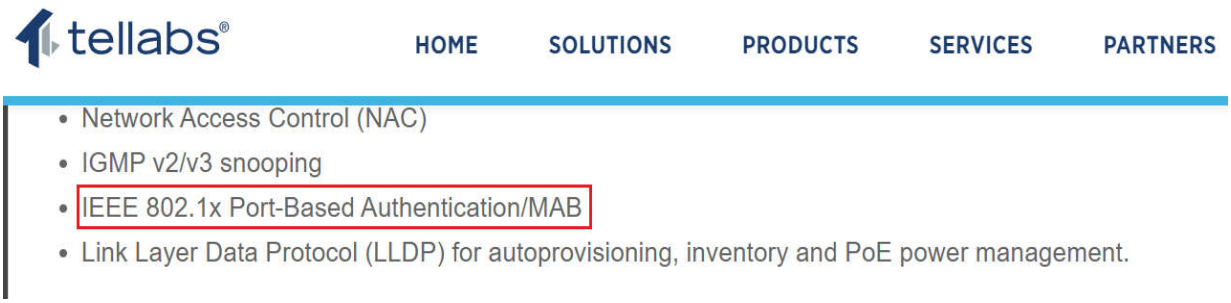
-> By using Authentication Timeout Switch knows whether the end device which is connected to an interface is having 802.1x supplicant or not.

-> By default Switch sends EAP request identity messages every 30 seconds to the endpoint, if the switch does not receive the response for three EAP request identity messages (90 seconds) then it assumes the host is not having 802.1x supplicant and begins MAB process.

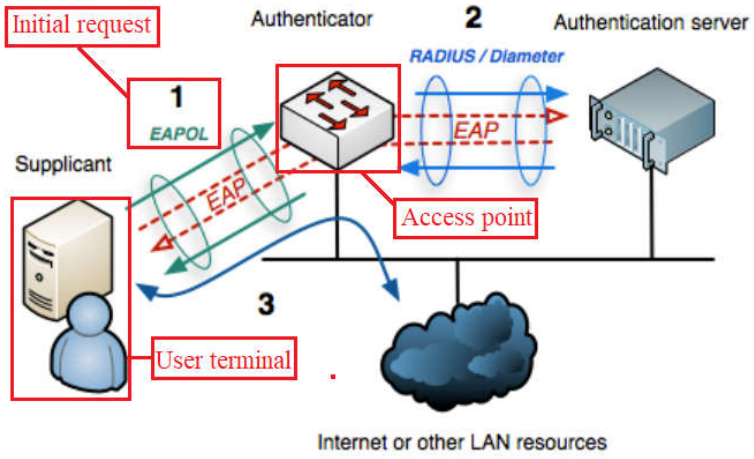
-> It is recommended to change the Authentication timeout period to less value.

(*E.g.*, https://www.kareemccie.com/2017/01/mac-authentication-bypass.html).

17. Upon information and belief, the access point determines that the user terminal is not IEEE 802.1x compliant when it does not receive an extensible authentication protocol identity (*e.g.*, response to the EAPoL request) response packet after a timeout value.



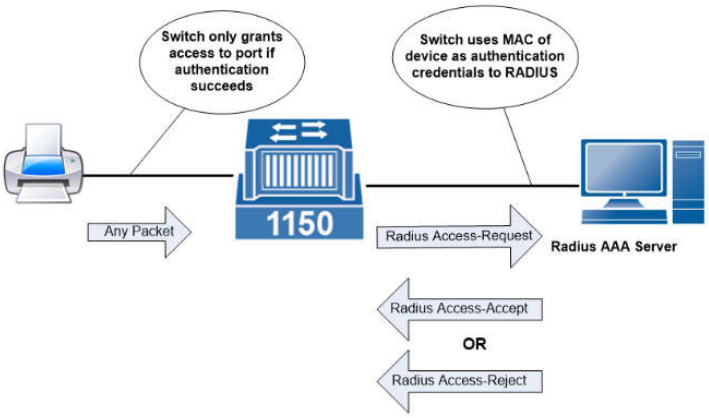
(*E.g.*, https://www.tellabs.com/product/ont205).



802.1X authentication involves three parties: a *supplicant*, an *authenticator*, and an *authentication server*. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.

(*E.g.*, https://docs.tellabs.com/articles/#!optical-lan-application-notes-publication/eng-010428-configuring-policy-via-radius-authenticationv4).

MAC Authentication Bypass Described



Many Enterprise and other secure installations use the 802.1x Port Authentication feature to control access to the Ethernet ports within a facility. The 802.1x protocol forces a user to authenticate using their credentials prior to gaining access to a port. The user is typically authenticated to some backend system such as RADIUS.

For many intelligent devices that support 802.1x this works well to secure the ports for use only by authorized parties. The problem is that there are simple devices such as printers and cameras that may not support 802.1x and backend authorization. In order to handle these use cases, the feature of MAC Authentication Bypass or MAB uses the MAC address of the attached device to authenticate to the backend AAA server, typically RADIUS.

Mixing of 802.1x and MAB

MAB and 802.1x can both be configured onto the port. The default settings will allow 802.1x to be tried first, followed by an attempt with MAB using the device's MAC address. An entire site can be configured this way to allow the 802.1x or MAB devices to be plugged into any port on the OLT. This can also be used for example to authenticate phones that don't support 802.1x but force PCs to authenticate.

It should be noted that if multiple devices are attempting access on the same port the 802.1x supplicants will ALWAYs be given preference over MAB clients.

(*E.g.*, https://docs.tellabs.com/articles/#!optical-lan-application-notes-publication/eng-010469-mac-authentication-bypass).

To enable MAB you need to change the following settings in the NAC profile:

- **MAC-BYPASS** – Should be set to enabled to turn on MAC Bypass.
- **Startup Delay** – Defaults to 30 seconds to give standard 802.1x time to complete prior to MAB being attempted. Always best to let 802.1x be attempted first, but some devices may need a shorter timer to speed up access to the network.
- **Authentication Method** – Set to PAP if your Radius server is set up to accept PAP.

(*E.g.*, https://docs.tellabs.com/articles/#!optical-lan-application-notes-publication/eng-010469-mac-authentication-bypass).

Authentication Timeout in 802.1x

-> By using Authentication Timeout Switch knows whether the end device which is connected to an interface is having 802.1x supplicant or not.

-> By default Switch sends EAP request identity messages every 30 seconds to the endpoint, if the switch does not receive the response for three EAP request identity messages (90 seconds) then it assumes the host is not having 802.1x supplicant and begins MAB process.

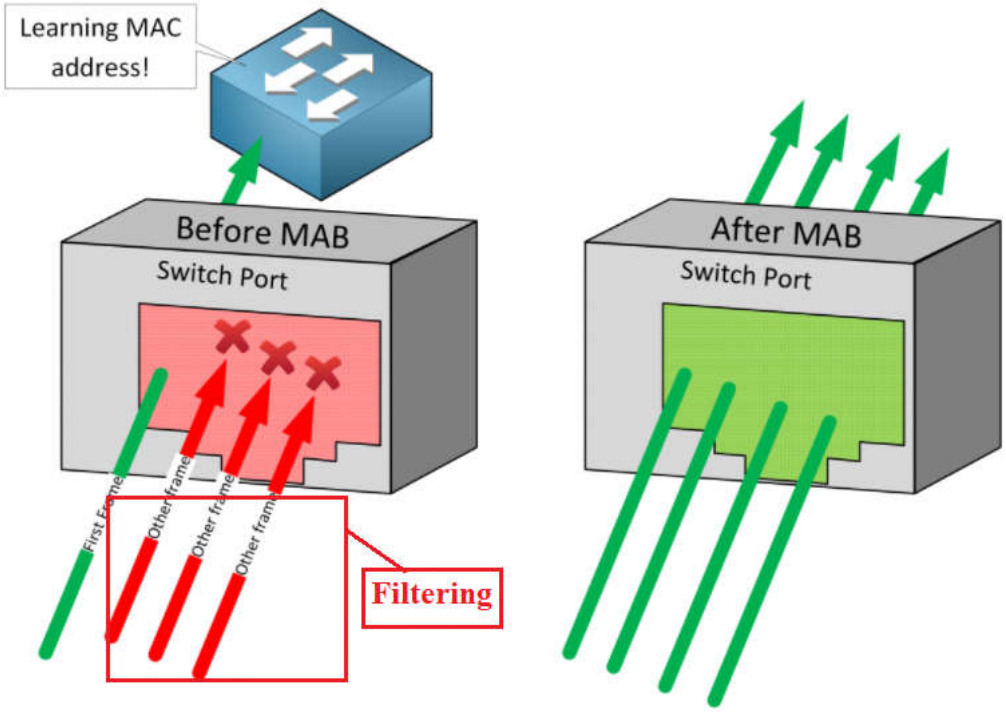
-> It is recommended to change the Authentication timeout period to less value.

(*E.g.*, https://www.kareemccie.com/2017/01/mac-authentication-bypass.html).

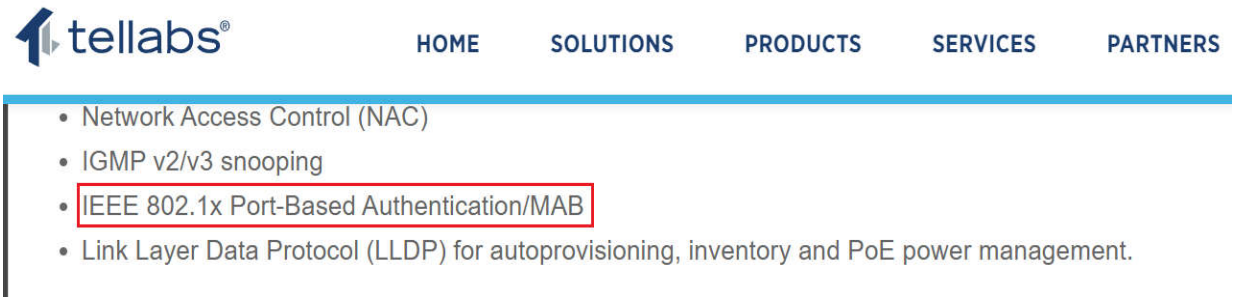
18. Upon information and belief, the Accused Instrumentality is used in a method performing the step of the access point detects if the user terminal is not IEEE 802.1x compliant, then configuring an internet protocol packet filter (*e.g.*, switch drops all the frames except the first frame to learn the MAC address) and redirecting a user request to a local server (*e.g.*, authentication server).

If you can't use 802.1X but still want to secure your switch ports somehow, you can use **MAC Authentication Bypass (MAB)**.

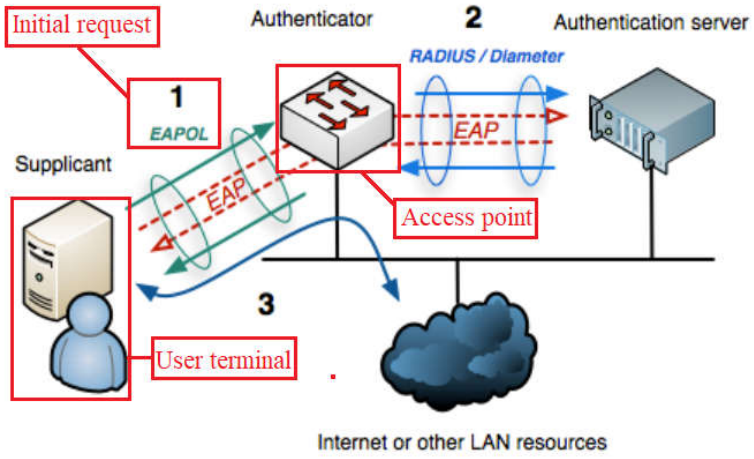
When you enable MAB on a switchport, the switch drops all drops all frames except for the first frame to learn the MAC address. Pretty much any frame can be used to learn the MAC address except for CDP, LLDP, STP, and DTP traffic. Once the switch has learned the MAC address, it contacts an authentication server (RADIUS) to check if it permits the MAC address.



(*e.g.*, https://networklessons.com/cisco/ccie-routing-switching-written/mac-authentication-bypass-mab#:~:text=Once%20the%20switch%20has%20learned,you%20can%20with%20802.1X.).



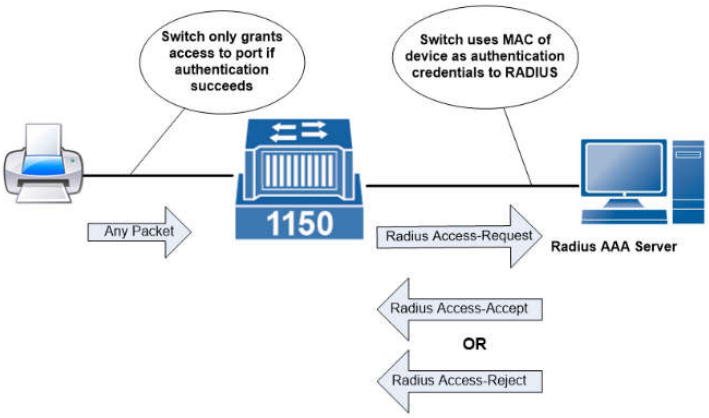
(*E.g.*, https://www.tellabs.com/product/ont205).



802.1X authentication involves three parties: a *supplicant*, an *authenticator*, and an *authentication server*. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.

(*E.g.*, https://docs.tellabs.com/articles/#!optical-lan-application-notes-publication/eng-010428-configuring-policy-via-radius-authenticationv4).

MAC Authentication Bypass Described



Many Enterprise and other secure installations use the 802.1x Port Authentication feature to control access to the Ethernet ports within a facility. The 802.1x protocol forces a user to authenticate using their credentials prior to gaining access to a port. The user is typically authenticated to some backend system such as RADIUS.

For many intelligent devices that support 802.1x this works well to secure the ports for use only by authorized parties. The problem is that there are simple devices such as printers and cameras that may not support 802.1x and backend authorization. In order to handle these use cases, the feature of MAC Authentication Bypass or MAB uses the MAC address of the attached device to authenticate to the backend AAA server, typically RADIUS.

Mixing of 802.1x and MAB

MAB and 802.1x can both be configured onto the port. The default settings will allow 802.1x to be tried first, followed by an attempt with MAB using the device's MAC address. An entire site can be configured this way to allow the 802.1x or MAB devices to be plugged into any port on the OLT. This can also be used for example to authenticate phones that don't support 802.1x but force PCs to authenticate.

It should be noted that if multiple devices are attempting access on the same port the 802.1x supplicants will ALWAYs be given preference over MAB clients.

(*E.g.*, https://docs.tellabs.com/articles/#!optical-lan-application-notes-publication/eng-010469-mac-authentication-bypass).

To enable MAB you need to change the following settings in the NAC profile:

- **MAC-BYPASS** – Should be set to enabled to turn on MAC Bypass.
- **Startup Delay** – Defaults to 30 seconds to give standard 802.1x time to complete prior to MAB being attempted. Always best to let 802.1x be attempted first, but some devices may need a shorter timer to speed up access to the network.
- **Authentication Method** – Set to PAP if your Radius server is set up to accept PAP.

(*E.g.*, https://docs.tellabs.com/articles/#!optical-lan-application-notes-publication/eng-010469-mac-authentication-bypass).

Authentication Timeout in 802.1x

-> By using Authentication Timeout Switch knows whether the end device which is connected to an interface is having 802.1x supplicant or not.

-> By default Switch sends EAP request identity messages every 30 seconds to the endpoint, if the switch does not receive the response for three EAP request identity messages (90 seconds) then it assumes the host is not having 802.1x supplicant and begins MAB process.

-> It is recommended to change the Authentication timeout period to less value.

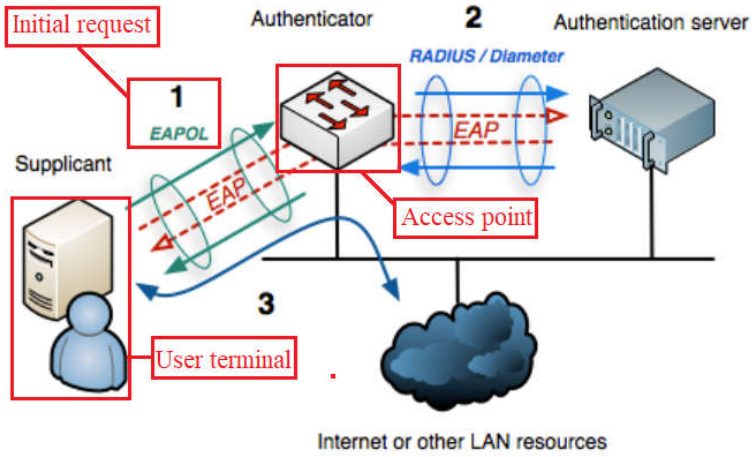
(*E.g.*, https://www.kareemccie.com/2017/01/mac-authentication-bypass.html).

19. Upon information and belief, the Accused Instrumentality is used in a method performing the step of the access point transitions (*e.g.*, from normal 802.1x authentication protocol after time out) to a state corresponding to browser based authentication (*e.g.*, authentication using RADIUS protocol via MAB) protocol if the user terminal is not IEEE 802.1x compliant.

tellabs® HOME SOLUTIONS PRODUCTS SERVICES PARTNERS

- Network Access Control (NAC)
- IGMP v2/v3 snooping
- IEEE 802.1x Port-Based Authentication/MAB
- Link Layer Data Protocol (LLDP) for autoprovisioning, inventory and PoE power management.

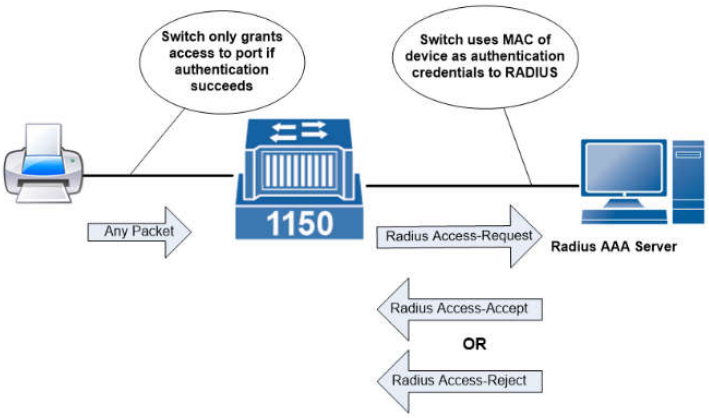
(*E.g.*, https://www.tellabs.com/product/ont205),



802.1X authentication involves three parties: a *supplicant*, an *authenticator*, and an *authentication server*. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.

(*E.g.*, https://docs.tellabs.com/articles/#!optical-lan-application-notes-publication/eng-010428-configuring-policy-via-radius-authenticationv4).

MAC Authentication Bypass Described



Many Enterprise and other secure installations use the 802.1x Port Authentication feature to control access to the Ethernet ports within a facility. The 802.1x protocol forces a user to authenticate using their credentials prior to gaining access to a port. The user is typically authenticated to some backend system such as RADIUS.

For many intelligent devices that support 802.1x this works well to secure the ports for use only by authorized parties. The problem is that there are simple devices such as printers and cameras that may not support 802.1x and backend authorization. In order to handle these use cases, the feature of MAC Authentication Bypass or MAB uses the MAC address of the attached device to authenticate to the backend AAA server, typically RADIUS.

Mixing of 802.1x and MAB

MAB and 802.1x can both be configured onto the port. The default settings will allow 802.1x to be tried first, followed by an attempt with MAB using the device's MAC address. An entire site can be configured this way to allow the 802.1x or MAB devices to be plugged into any port on the OLT. This can also be used for example to authenticate phones that don't support 802.1x but force PCs to authenticate.

It should be noted that if multiple devices are attempting access on the same port the 802.1x supplicants will ALWAYs be given preference over MAB clients.

(*E.g.*, https://docs.tellabs.com/articles/#!optical-lan-application-notes-publication/eng-010469-mac-authentication-bypass).

To enable MAB you need to change the following settings in the NAC profile:

- **MAC-BYPASS** – Should be set to enabled to turn on MAC Bypass.
- **Startup Delay** – Defaults to 30 seconds to give standard 802.1x time to complete prior to MAB being attempted. Always best to let 802.1x be attempted first, but some devices may need a shorter timer to speed up access to the network.
- **Authentication Method** – Set to PAP if your Radius server is set up to accept PAP.

(*E.g.*, https://docs.tellabs.com/articles/#!optical-lan-application-notes-publication/eng-010469-mac-authentication-bypass).

Authentication Timeout in 802.1x

-> By using Authentication Timeout Switch knows whether the end device which is connected to an interface is having 802.1x supplicant or not.

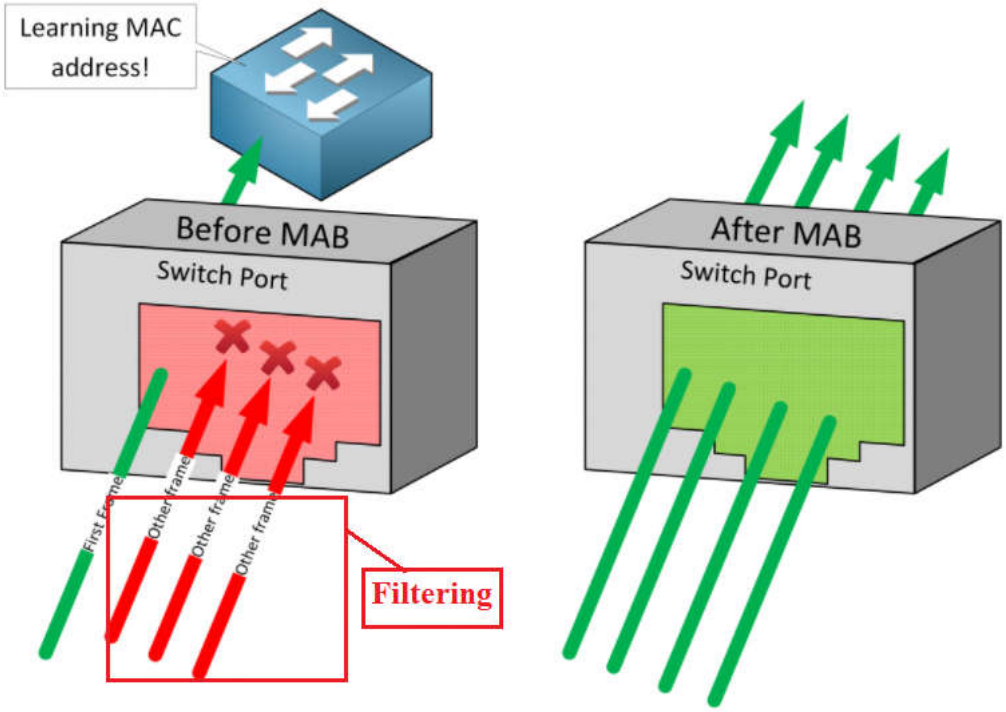
-> By default Switch sends EAP request identity messages every 30 seconds to the endpoint, if the switch does not receive the response for three EAP request identity messages (90 seconds) then it assumes the host is not having 802.1x supplicant and begins MAB process.

-> It is recommended to change the Authentication timeout period to less value.

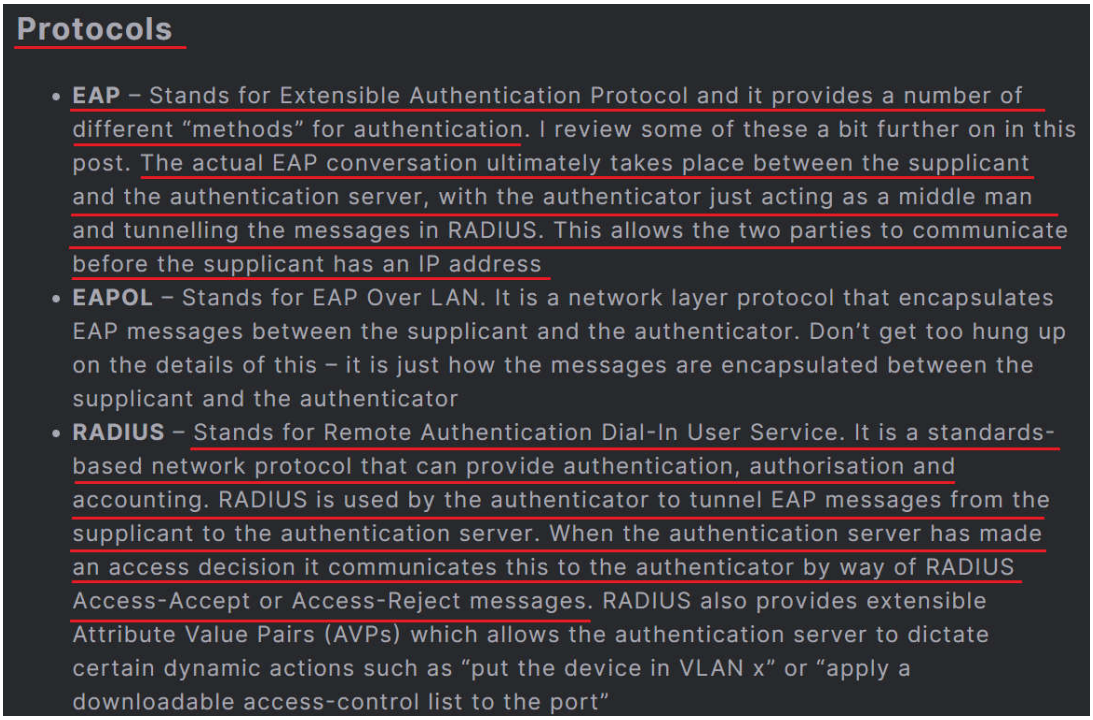
(*E.g.*, https://www.kareemccie.com/2017/01/mac-authentication-bypass.html).

If you can't use 802.1X but still want to secure your switch ports somehow, you can use **MAC Authentication Bypass (MAB)**.

When you enable MAB on a switchport, the switch drops all drops all frames except for the first frame to learn the MAC address. Pretty much any frame can be used to learn the MAC address except for CDP, LLDP, STP, and DTP traffic. Once the switch has learned the MAC address, it contacts an authentication server (RADIUS) to check if it permits the MAC address.



(*e.g.*, https://networklessons.com/cisco/ccie-routing-switching-written/mac-authentication-bypass-mab#:~:text=Once%20the%20switch%20has%20learned,you%20can%20with%20802.1X.).



Protocols

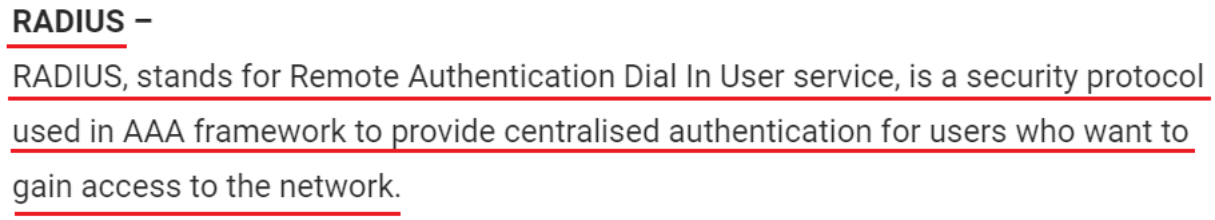
- **EAP** – Stands for Extensible Authentication Protocol and it provides a number of different "methods" for authentication. I review some of these a bit further on in this post. The actual EAP conversation ultimately takes place between the supplicant and the authentication server, with the authenticator just acting as a middle man and tunnelling the messages in RADIUS. This allows the two parties to communicate before the supplicant has an IP address
- **EAPOL** – Stands for EAP Over LAN. It is a network layer protocol that encapsulates EAP messages between the supplicant and the authenticator. Don't get too hung up on the details of this – it is just how the messages are encapsulated between the supplicant and the authenticator
- **RADIUS** – Stands for Remote Authentication Dial-In User Service. It is a standards-based network protocol that can provide authentication, authorisation and accounting. RADIUS is used by the authenticator to tunnel EAP messages from the supplicant to the authentication server. When the authentication server has made an access decision it communicates this to the authenticator by way of RADIUS Access-Accept or Access-Reject messages. RADIUS also provides extensible Attribute Value Pairs (AVPs) which allows the authentication server to dictate certain dynamic actions such as "put the device in VLAN x" or "apply a downloadable access-control list to the port"

(*E.g.*, https://mikeguy.co.uk/posts/2018/06/understanding-nac-802.1x-and-mab/).

Introduction

The Remote Authentication Dial-In User Service (RADIUS) protocol was developed by Livingston Enterprises, Inc., as an access server authentication and accounting protocol. The RADIUS specification RFC 2865 leavingcisco.com obsoletes RFC 2138. The RADIUS accounting standard RFC 2866 leavingcisco.com obsoletes RFC 2139.

(*E.g.*, https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html).



RADIUS –

RADIUS, stands for Remote Authentication Dial In User service, is a security protocol used in AAA framework to provide centralised authentication for users who want to gain access to the network.

(*E.g.*, https://www.geeksforgeeks.org/radius-protocol/).

20. Defendant's customers also infringe claims 9, 10, and 11 of the '037 patent by using or performing the claimed method using the Accused Instrumentality as described above. Furthermore, Defendant advertises, markets, and offers for sale the Accused Instrumentality to its

customers for use in a system in a manner that, as described above, infringes claims 9, 10, and 11 of the '037 patent. Exemplary materials are cited above.

21. Plaintiff has been damaged as a result of Defendant's infringing conduct. Defendant is thus liable to Plaintiff for damages in an amount that adequately compensates Plaintiff for such Defendant's infringement of the '037 patent, *i.e.*, in an amount that by law cannot be less than would constitute a reasonable royalty for the use of the patented technology, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

22. The asserted claims of the '037 Patent are method claims to which the marking requirements are not applicable. To the extent required, Plaintiff has therefore complied with the marking statute.

IV. JURY DEMAND

Plaintiff, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

V. PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court find in its favor and against Defendant, and that the Court grant Plaintiff the following relief:

a. Judgment that one or more claims of United States Patent No. 8,272,037 have been infringed, either literally and/or under the doctrine of equivalents, by Defendant;

b. Judgment that Defendant account for and pay to Plaintiff all damages to and costs incurred by Plaintiff because of Defendant's infringing activities and other conduct complained of herein;

c. That Plaintiff be granted pre-judgment and post-judgment interest on the damages caused by Defendant's infringing activities and other conduct complained of herein;

d. That Plaintiff be granted such other and further relief as the Court may deem just and proper under the circumstances.

August 31, 2022

NI, WANG & MASSAND, PLLC

/s/ Hao Ni
Hao Ni
8140 Walnut Hill Lane, Suite 500
Dallas, TX 75231
Telephone: (972) 331-4600
Email: hni@nilawfirm.com

Attorneys for Plaintiff Tranquility IP LLC

OF COUNSEL:

David R. Bennett
Direction IP Law
P.O. Box 14184
Chicago, IL 60614-0184
(312) 291-1667
dbennett@directionip.com